LEX PROSPICIT
Volume 2 Issue 2 July 2024
P-ISSN: 2988-1781, E-ISSN: 2988-1773

THE IMPACT OF TECHNOLOGY ON PERSONAL DATA PRIVACY AND SECURITY LAW: A CRITIQUE OF THE NATIONAL LEGAL FRAMEWORK (CASE STUDY OF BANK SYARIAH INDONESIA CUSTOMER DATA LEAK)

Florentina Dani Eti Kusuma Eko Wardani[1], R. Febriarto Fadjar[2*], Mychelvia Vrelya Giovanni Latuhihin[3]

[1, 3] Faculty of Law Universitas Pelita Harapan, Indonesia
[2] Legal & Compliance Department PT Zurich Topas Life, Indonesia

email: febriarto.fadjar@zurich.co.id
(Corresponding Author indicated by an asterisk *)

Article Info

Article History:
Submitted: 20 February 2024
Revised: 22 July 2024
Published: 31 July 2024

Keywords:
Privacy Law; Data Protection; Development of National Data Security Law

DOI:
http://dx.doi.org/10.1966/lp.v2i2.8021

Abstract

Technological developments require humans as personal data subject entities or personal data owners to submit various personal information to personal data controllers to be able to carry out certain activities. This is the impact of technological developments which are known to have no limits and space in connecting other humans with other humans by only conveying some information to themselves. This research uses normative juridical research with a statutory approach and a case approach. The leak of personal data belonging to Bank Syariah Indonesia customers in May 2023 is proof that the Personal Data Controller (Bank Syariah Indonesia) is responsible for its customers. In its implementation, the Government in this case has established Law Number 27 of 2022 on Personal Data Protection and its implementing regulations for data protection and security. However, in fact, the law or implementing regulations have not been effective enough to be implemented perfectly in resolving the problem of data leakage and still violate the privacy rights of citizens (especially BSI Bank customers). In the positive law that has been implemented (Personal Data Protection Law), the first form of implementation of legal responsibility that must be carried out by the Personal Data Controller when personal data is leaked is to provide written notification no later than 3x24 hours if there is a failure to protect personal data to the personal data subject and also agencies.

1. INTRODUCTION

The State of Indonesia is a concept of a state designed to be a state of law. As a state of law, Indonesia is obliged to fulfill and carry out every legal consequence in providing and guaranteeing human rights for all citizens without exception. One of the guarantees that must be given by the state is related to a healthy environment. It is also stated in the 1945 Constitution of the Republic of Indonesia that all Indonesian citizens are entitled to proper protection from actions or threats that make themselves insecure and make their lives

disrupted by others.[1] Not only that, problems in the implementation of providing protection to citizens are also sought in the form of a version in the constitution.

The government as a neutral subject of law must be able to provide protection for its citizens. The concept of legal protection that is then expected and promulgated by the state is a concept of legal protection that is preventive (before the occurrence of events) or legal consequences (repressive legal protection). Humans are known as a unity in a community group, have 2 aspects, namely the human aspect which is seen as a unity of individuals and also the human aspect which is seen as having a relationship between humans and other humans (social relations). Talking about the human aspect as an individual, we will see humans who have egocentric towards themselves over others around them. Meanwhile, when talking about humans from the point of view of aspects of human relations with other humans (social relations), it will be reflected and created the importance of a norm that must live among them. These norms will form a system that will create a sense of justice for every society.

Telematics legal terminology in this case has a broader study with the existence of cyber law. This can be seen from the understanding of telematics law which explains that the whole of the norms, rules, and principles of information technology which in this case is packaged into one unit. If you look at the formulation of this understanding, it can be concluded that cyber law in this case is also part or derivative of telematics law. Telematics law and cyber law are intrinsically inseparable from each other, interrelated, but when examined more deeply, cyber law and telematics law are different objects of legal study.[2] Cyber law is defined as all aspects that have a relationship between legal subjects and legal subjects who use and utilize technology as a medium or intermediary in cyberspace.[3] The existence of a relationship and activities in cyberspace cannot be separated from the existence of telematics laws which basically discuss technology and cyberspace. Telematics law and cyber law in this case are included in a study group of technology law and the development of digitalization.

The development of Big Data illustrates the astonishing increasing growth, availability and utilization of information in today's world. The ever-increasing volume of unstructured structures and information, its diversity, and the speed with which it is generated, through social media, censors data as well as transaction data, poses today's leaders and specialists with increasing nefarious opportunities and challenges. With Big Data benefiting from increased storage capabilities, thinking is moving away from what records to keep to ponder the question of how to make sense of these large volumes of data.[4] The Big Data market is in its nascent stage and is expected to expand as companies as well as public bodies seek to increase their competitive advantage by better understanding the growing amount of data. Artificial intelligence offers the technology and methodology to do so, and the market for artificial intelligence-based tools and applications is growing rapidly. The uptake of this trend could benefit European companies as well as the EU economy and labor

---

1 The 1945 Constitution of the Republic of Indonesia.

2 Mohd. Safar Hasim, *Mengenali Undang-Undang Media dan Siber [Regarding Media and Cyber Law]* (Kuala Lumpur: Utusan Publications & Distributions, 2002), 118.

3 Sahat Maruli T. Situmeang, *Cyber Law* (Jakarta: Cakra, 2020), 14.

4 Mubashir Hussain and Jatinder Manhas, "Artificial Intelligence for Big Data: Potential and Relevance," *International Academy of Engineering and Medical Research* 1, no. 1 (2016): 1, https://www.researchgate.net/publication/310447985.

market, as the development and management of artificial intelligence requires highly skilled workers in many areas.[5]

Data plays an important role in the world of economics business, especially in the digital economy. Data is collected, processed, and commercially exploited by large corporations. Data becomes an asset that determines the company's strategy in competition. The need for Big Data is closely related to the merger and acquisition process of the technology and communication sector where aspects of consumer privacy can be perceived as relevant to aspects of non-price competition parameters in measuring the impact of competition. For example, in the case of the Microsoft/LinkedIn merger, the European Commission (EC) ruled that although customers' privacy rights are governed by data protection laws, the EC is of the opinion that this aspect falls under the category of non-price competition factors in merger control assessments when it concludes that consumers see this aspect as a significant factor that will determine the services provided. Data is one of the important aspects that must then be given legal certainty by the government. This then requires the state to be present in the formation of national laws in providing legal certainty for data protection.

Currently, the Indonesian government has been present in forming a national law on personal data protection for citizens through Law Number 27 of 2022 on Personal Data Protection. Then, it is also explained in the implementing rules through Regulation of Minister of Communication and Information Number 20 of 2016 on Personal Data Protection in Electronic Systems. However, it is undeniable that until now there are still many cases of personal data leakage which then provide urgency for the country. This then becomes a separate question of how the national law applied today can be used as a tool for personal data protection for citizens and create legal certainty.

The problem that the author raises relates to actions that are considered unlawful committed by Corporations that commit negligent acts and cause consumers to lose money due to the leakage of personal data against their companies.[6] Actions that are considered against the law also provide a problem that it is proven that personal data belonging to consumers and also business actors who are members of it are traded in black shops or in a black market shop. This is then considered to be able to cause a loss for consumers and business actors need to take responsibility for these actions. As the case occurred in Bank Syariah Indonesia (hereinafter referred to as BSI) has been negligent in safeguarding personal data belonging to its customers and was successfully hacked by hackers and a failed mediation process that caused hackers to spread BSI customer data traded on the black market. As explained in Article 1 Number 4 of Law Number 27 of 2022 on Personal Data Protection (hereinafter referred to as the PDP Law), personal data controllers are those who belong to persons, public bodies or international organizations who then act alone or simultaneously in determining a purpose for a personal data process. BSI towards its customers here is referred to as the controller of personal data whose obligations include maintaining and ensuring the data of the subject of the data owner is stored safely.

With the existence of BSI committing violations of personal data belonging to customers, in this case BSI must be legally responsible for losses experienced by its customers. BSI is one of the mergers of Islamic banks in which then has committed actions

---

5 *Ibid.*, 2.

6 Siti Yuniarti, "Perlindungan Hukum Data Pribadi di Indonesia [Legal Protection of Personal Data in Indonesia]," *Business Economic, Communication, and Social Sciences Journal (BECOSS)* 1, no. 1 (2019): 151, https://doi.org/10.21512/becossjournal.v1i1.6030.

that are considered against the law with the leakage of customer personal data stored by BSI itself. The purpose of this research is to examine how the national legal system and positive laws applied in Indonesia can provide protection to citizens for their right to privacy.

2. METHOD

The type of method used in this study is the normative legal research method. The normative legal research method is a procedure to find rule of law, legal principles, and legal doctrines to answer legal problems.[7] The approach used in this study is statutory approach or statute approach, which is an approach through the use of legislation and regulations and also pays attention to the hierarchy and principles in laws and regulations.[8] This research uses a conceptual approach because one part of this research will later begin by identifying existing principles or doctrinal views to then bring up new ideas. This normative legal research is descriptive as part of legal science activities to explain the law. Only facts that become primary legal material to explain the law and make decisions about the law of the legal field.[9]

3. RESULTS AND DISCUSSION

3.1 Analysis of Legal Arrangements Regarding Legal Events of Personal Data Leakage Conducted by BSI in the Aspects of Personal Data Protection and Consumer Protection

Telematics law is defined as a word for cyber law which is then used internationally for legal terms related to the use of information technology.[10] Telematics law is the entire principles, norms, or rules of institutions implemented in this case using all information and communication technology. Telematics law and cyber law are essentially the same but cannot be equated, the equation is essentially related to technology and communication. But in this case cyber law is an inseparable part of telematics law (a derivative of the telematics law). The scope of cyber law in this case only covers aspects that have relationships with individuals or other legal subjects who use internet technology starting in cyberspace.[11] This then causes cyber law in this case to be narrower in scope compared to telematics law. This then gives a consequence that the operation of commercial business in the telecommunications and broadcasting subsector requires taking care of licensing. It is necessary to regulate the licensing process because in the telecommunications sector there are many business actors and interests. There needs to be restrictions from business actors in the telecommunications sector to regulate, limit, and provide regulations. Unlike the case with informatics applications which in this case are disseminated and used in the field of digital media. The use of media in this case is only limited to ethics in conducting and using

---

7 Mukti Fajar ND, and Yulianto Achmad, *Dualisme Penelitian Hukum Normatif & Empiris [Dualism of Normative and Empirical Legal Research]* (Yogyakarta: Pustaka Belajar, 2015), 34.

8 Peter Mahmud Marzuki, *Penelitian Hukum [Legal Research]* (Jakarta: Kencana, 2007), 137.

9 Prapti Rahayu Derita, *Metode Penelitian Hukum [Legal Research Methods]* (Yogyakarta: Thafa Media, 2020), 87.

10 Ahmad M. Ramli, *Cyber Law and HAKI dalam Sistem Hukum Indonesia [Cyber Law and IPR in the Indonesian Legal System]* (Jakarta: Refika Aditama, 2020), 54.

11 Sahat Maruli T. Situmeang, *Op. Cit.*, 39.

informatics applications. Thus, between the implementation of commercial business in the telecommunications subsector and also the informatics application sector has a significant difference

The financial digital platform is a form of convenience in developing the digital economy.[12] However, if phishing crimes are not eradicated and not acted upon, then the digital economy will never be present in society if there is no technology to support it. Sometimes people are complacent with the convenience provided but forget about the dangers and possibilities that exist in a digital economic development. So, that's where the role and function of cyber law in society. Cyber law and its development in cyber security are expected to provide a form of solution in overcoming problems or crimes that may occur in the world of technology when running the digital economy, including phishing crimes.[13] Based on state defense theory, cyber law is used as a tool to provide state defense which is closely related to cyber defense and cyber security. Cyber law is needed to protect the rights of citizens in getting security for their transactions, most of which use internet banking applications that can be hacked by anyone.[14]

The government in countering cybercrime in this case must form a cyber defense force as a first step to prevent cybercrime in an agency or institution. It should be understood that cybercrime can happen to anyone. This then shows that the implementation of cybercrime in Indonesia must be prevented and tackled massively and structurally by all parties, both the government and also every person or entity that uses technology. Not only that, the disadvantage of cyber crime law enforcement is the lack of clear regulations regarding dispute resolution that occur. This is because litigation and non-litigation efforts are still unclear about the mechanisms applied to combat cybercrime.[15] Thus, there needs to be strengthening and clarity in the dispute resolution mechanism system for cybercrime cases needs to be improved by the government.

Cybercrime countermeasures policy with criminal law including the field of penal policy which is then part of criminal policy (crime reduction policy) can be used as an alternative.[16] As a form of high tech crime that can then cross national borders or transborder, it is also natural that an effort to overcome cybercrime must also be taken with a technological approach or techno prevention. Cybercrime enforcement must be handled seriously, because in its development the type, way, mechanism of everyone who seeks to commit cybercrime continues to develop and continues to look for loopholes in the system formed by the government. Not only regulations are encouraging, but each person, agency, or institution must also strengthen their respective security systems or cyber defense so that in tackling cybercrime this can be overcome or at least can be minimized. The mechanism for combating cybercrime needs to be carried out with the cooperation of all relevant stakeholders, both from the government side that issues specific regulations and regulates the implementation of cybercrime crimes and also the role of each individual or entity or institution that strengthens from the side of cyber defense as the main shield to strengthen

---

12 Assafa Endeshaw, *Hukum E-Commerce dan Internet dengan Fokus di Asia Pasifik [E-Commerce and Internet Law with a Focus on Asia Pacific]* (Surabaya: Bina Ilmu, 2007).

13 Richardus Eko Indrajit, *Cyber Resilience: A Holistic Strategy to Address Contemporary Defense Threats in Cyberspace* (Jakarta: BSSN, 2019).

14 Wahyudi Djafar and M. Jodi Santoso, "Personal Data Protection Recognizes the Rights of Data Subjects, as well as the Obligations of Data Controllers and Processors," *ELSAM Publication Journal* (2020): 8.

15 Sahat Maruli T. Situmeang, *Op. Cit.*

16 Edmon Makarim, *Kompilasi Hukum Telematika [Telematics Law Compilation]* (Jakarta: Raja Grafindo, 2003), 63.

the system for cybercrime do not damage the technological system or do not enter into the technological space owned by the individual or entity or institution.

The event of leakage of personal data in this case can be tied to the existence of an explanation of unlawful acts. According to Subekti, to be able to determine that an act is considered unlawful, the act causes harm to others due to his negligence, it is mandatory for him to pay compensation.[17] Acts that are considered unlawful are stipulated in Article 1365 of the Indonesian Civil Code, which explains every act that is considered unlawful that causes harm to others must provide compensation. To be able to say that an act is an unlawful act, it fulfills the following elements:

a. The existence of an action, that the action in question is to do something or not to do something. In this case, the act taken by BSI is to disseminate personal data belonging to BSI Users or in this case BSI customers;
b. This action violates the law, which in this case violates the applicable law with provisions regarding personal data protection for customers and also violates the subjective rights owned by customers or users of BSI in terms of their personal data rights;
c. There is an element of guilt, related to an act that in essence is not much different from the element of against the law. This element of guilt essentially applies to the provision of unlawful elements that can be used as a reason to hold someone responsible for an act he committed. Acts that contain elements of guilt can be held accountable. The mistake made is in the form of negligence in supervising the safeguarding of personal data and in this case no updates to the security of personal data belonging to customers;
d. There is a loss, in the event that the party harmed as a result of unlawful acts can file a lawsuit to the court. Users are immaterially harmed by the dissemination of their personal data;
e. There is a relationship between actions and losses. In this case, BSI Users or BSI customers suffer immaterial loss due to negligent actions caused by BSI itself. This is evidenced by the circulation of customer data from BSI which is traded on the black market by violators. Of course, the dissemination and circulation of BSI customer data is due to errors and omissions from BSI which does not update security.

So, it can be concluded that BSI have committed actions that are considered unlawful and caused losses to BSI Users, in this case BSI customers themselves who also use banking and financial facilities from BSI.

For the actions carried out by BSI, in this case, serious handling is needed because if it is not handled it will lead to new cases. Therefore, the competent authorities and the parties concerned, especially the Minister of Information and Communication and BSI, are obliged to provide solutions to the problems of losses experienced by BSI customers. Article 3 Regulation of Minister of Information and Communication Number 20 of 2016 on Personal Data Protection in Electronic Systems states that "protection of personal data in electronic systems is provided for any process of obtaining and collecting, processing and analyzing, storing, displaying, announcing, sending, disseminating, and/or opening access, and destruction."

---

[17] R. Subekti and R. Tjitrosudibio, *Kitab Undang-Undang Hukum Perdata [Indonesian Civil Code]* (Jakarta: Pradnya Paramitha, 2002).

Thus, BSI as a business entity must provide legal protection guarantees to BSI customers in every process of processing personal data. The legal protection obtained is related to the guarantee of the rights of BSI customers in terms of making dispute resolution efforts for losses suffered due to personal data leakage. Then, the guarantee that must be provided by BSI next is a guarantee of further protection for the management of personal data.

3.2 Development of National Law in Providing Protection of Personal Data Security of Citizens

Roscoe Pond explained that he divided the theory of interests into 3, namely individual interests, public interests, and social interests. According to Pound, the law must play a role in balancing each competing interest in society in order to achieve substantial profits.[18] Similarly, in relation to privacy, that what has been classified as privacy is not placed in the realm of privacy with the existence of the theory of interest. An example applied in Indonesia is in the banking sector if there is a state official who has indications of committing a criminal act of corruption, then the official authorized to investigate can access the banking account of the state official without seeking approval from the person concerned on public interest grounds (saving state money). Privacy theory is a map that shows that people make choices about disclosing or hiding private information based on criteria and conditions that are considered important, and they believe that they have the right to regulate access to that private information.[19] An example is in its application in Indonesia when we register for an e-commerce, that data that is essentially considered important we can give access to others to participate in storing and managing our privacy data.

Privacy is part of the human rights possessed by every human being which makes the basis that every human being has the right to association, thought, expression, get equal treatment. Then, in terms of privacy in the article is also based on the freedom to register intellectual property rights owned by certain people. Not only that, the article tries to explain the legal consequences given if there is a violation of privacy rights. If there is an element that constitutes a violation of legal injury, the elements to claim compensation are contained in it because there is already mental suffering caused by the act of violation of privacy and such compensation is considered compensation. Then privacy in the article is also interpreted as what a person has become entitled to and to prevent his public portrait, presenting the simplest case for such an extension; the right to protect oneself from a portrait of a pen, from discussion by the press of one's personal affairs, would be a more important and far-reaching right.

Then, privacy also has a relationship with technology. Technology and privacy are an inseparable whole. That in the current era of disruption using technology is a necessity and in accessing the technology users are asked to submit their privacy data. That vulnerability to privacy violations occurs because of technology. Privacy is a privacy exercise. Basically, the granting of privacy rights is the authority of the owner of the privacy. The fact is that in the current era, privacy data has spread hence there is technology on the internet. Then, the

---

[18] Shidarta, "The Role of the State in Responding to Investment According to the Theory of Interest of the Pound," *Binus University Business Law*, January 2016, https://business-law.binus.ac.id/2016/01/03/peran-negara-dalam-menyikapi-investasi-teori-kepentingan-pound/.

[19] Felicia Njotorahardjo, "Manajemen Komunikasi Privasi Seorang Mantan Pria Simpanan [Management of Privacy Communication of a Mistress]," *Jurnal E-Komunikasi* 2, no. 3 (2014): 1, https://publication.petra.ac.id/index.php/ilmu-komunikasi/article/view/3813.

relationship created between privacy and technology is also based on the fact that these two things are inseparable and cannot stand alone for those who use technology facilities. At this time, when someone uses technology, privacy about ourselves when using or enjoying technology services is directly known and recorded. Therefore, the trend is the need for protection of the right to privacy for every technology user on the internet.

The definition of personal data can be found in the Regulation of Minister of Communication and Information Technology Number 20 of 2016 on Personal Data Protection in Electronic Systems. Based on Article 1 Numbers 1 and 2, personal data is defined as any true and real personal data attached to and identifiable to that person, certain individual data that is stored, maintained, and maintained truthfully and protected confidentially.[20] Then, personal data protection is regulated under Article 2 Paragraph (1) of Regulation of Minister of Communication and Information Technology concerning Personal Data Protection in Electronic Systems which stipulates that Personal Data Protection in Electronic Systems includes protection against the acquisition, collection, processing, analysis, storage, display, announcement, transmission, dissemination, and destruction of Personal Data. Then, personal data protection must also follow the principles of personal data protection that respect personal data as privacy. The latest issue in recent times is that the PeduliLindungi application turns out to violate human rights in terms related to the protection of citizens' personal data.

Not only that, in this case the government has created data protection arrangements implied in it in Government Regulation Number 80 of 2019 on Trading Through Electronic Systems (Perdagangan Melalui Sistem Elektronik/PMSE) is a regulation made to adjust the times that are affected by technology. It can be seen in the provisions of Article 2 of this Government Regulation[21] which explains that the scope of the regulation of this legal product is related to parties carrying out activities in PMSE, related to the requirements and procedures imposed in transactions through PMSE, the implementation and also the governance of PMSE applied, the obligations of business actors when carrying out PMSE activities, related to the proof process through the proof of transaction process at PMSE, arrangements regarding advertisements submitted to electronic media or electronic advertising, other content materials regulate offering, acceptance, and also providing confirmation electronically, then related to electronic contracts, relating to the concept of protection of personal data, the process of sending goods and services in PMSE. There is a form of responsibility in the implementation of the exchange or refund of goods or services, dispute resolution processes that are carried out and can be used, and regulate the central role of the government, protection of personal data for users of electronic transaction services, and law enforcement related to guidance and supervision.[22]

Rules related to the legal protection of personal data have become the focus of the government. One of the reasons why it is important for one's personal data to be protected is that one's personal data can provide economic value to those who master it. To provide protection and strengthen the argument that personal data has economic value. In the news conveyed by Ministry of Home Affairs that wants to collect a fee of Rp1,000, it shows the government's unreadiness to protect personal data belonging to its citizens even though it is only in the form of NIK. We know that NIK is a very important number and needs to be kept confidential because it can be misused. My opinion in this case will be strengthened

---

20 Siti Yuniarti, *Loc. Cit.*, 147.

21 Article 2 *Government Regulation Number 80 of 2019 on Trading Through Electronic Systems.*

22 Elucidation of *Government Regulation Number 80 of 2019 on Trading Through Electronic Systems.*

from 2 sides, namely with regard to personal subject data rights and also the principle of accountability.

The personal data subject has the right to obtain information from the data controller in a transparent, complete and easily accessible manner, using clear and understandable language with regard to the processing of personal data, at the time the personal data is obtained, if the personal data was obtained not directly from the data subject, or within a reasonable period of time after obtaining the personal data, but no later than within one month if the personal data was obtained from the source other.[23] Without the need to provide a penny, every owner of personal data has the right to get access to information about his NIK number. This is also supported by Article 2 Paragraph (2) Letter i of Regulation of Minister of Communication and Information Number 20 of 2016 on Personal Data Protection in Electronic Systems which also emphasizes the necessity in the ease of accessing personal data so that the government is obliged to accommodate it and realize it. Regarding the principle of accountability with regard to efforts to realize other personal data protection principles as a step that has an impact on the principles mentioned in point number 1. When the government is not ready to provide access to support personal data protection facilities, it means that the government is not ready to provide personal data protection to its citizens. Providing a small fee shows the government's inability to manage and maintain and create conditions for personal data protection for its citizens.

The number of cyber-attacks that caused losses to citizens also occurs in virus attacks carried out by irresponsible individuals, such as the WannaCry ransomware attack. In Indonesia, the national legal framework to overcome WannaCry ransomware attack is regulated in the provisions of Law Number 19 of 2016 on Amendments to Law Number 11 of 2008 on Electronic Information and Transactions. The law describes the existence of an act and event which on average regulates the activities of a network or on the internet or in cyberspace. Not only Law Number 19 of 2016, but in the Criminal Code, Telecommunications Law has also regulated and explained the regulation of virus attacks in the cyber world.[24] As is known that in implementing and overcoming the problem of ransomware crime, Indonesia adopts the provisions contained in the Convention on Cybercrime which was incorporated into Law Number 19 of 2016 on Amendments to Law Number 11 of 2008 on Electronic Information and Transactions as material content for cybercrimes.

Then, investigating virus crimes and also the development of personal data in this case is also regulated in several countries. This can be seen in the rules and regulations of China and the European Union. The development of practices in the two countries is as follows:

ELEMENTS	Comparison of Personal Data Settings	
	CHINA	EUROPEAN UNION
Legal Subjects	State-Owned Enterprises, Private-Owned Enterprises are required to reduce data collection and require user consent.	A person of sufficient age or a Legal Entity including International Organizations that are considered legally capable, namely member states of the European Union.

[23] Wahyudi Djafar and M. Jodi Santoso, *Loc. Cit.*, 8.

[24] Andi Rian Jubhari, "Tinjauan Hukum Pidana Internasional Terhadap Serangan Siber Menggunakan Virus Ransomware WannaCry di Indonesia [International Criminal Law Analysis of Cyberattacks Using Wannacry Ransomware Virus in Indonesia]" (Undergraduate Thesis, Universitas Hasanuddin, 2022), Hasanuddin Repository, https://repository.unhas.ac.id/id/eprint/12272/.

Purpose	To protect those who feel secure about a storage of personal data used for user profiles and also with the algorithm of recommendations or the use of big data in setting a price.	To provide an extra protection to a data privacy in the development of the digital economy and protect personal data universally.
Organized Objects	Prevent companies from setting different prices for the same service based on the client's shopping history.	Regulate the protection of personal data of all EU citizens who have transaction relations with the territory of other countries or within the country. Not only prioritizing economic activities.
The role of the state	Provide special protection to every consumer, producer, and activity related to economic transactions. The State has the right to impose obligations and prohibitions on any data transfers made.	In each country the EU provides at least one public body to ensure oversight of the implementation of this regulation, as well as provide assistance to data owners. In its formation, the body can be formed by the government transparently, both by the legislature and the executive.
Penalty	Sanctions stipulated in the Personal Data Disclosure in China are subject to a fine of 1 million Yuan or equivalent to 2.2 billion for those who violate it.	The sanctions given and regulated in this case are administrative fines up to EUR 10,000,000 to EUR 20,000,000. Even criminal sanctions can also be included in the prosecution.
EQUATION	Personal data arrangements in China and Europe both provide arrangements regarding the protection of economic actors. The first purpose of making it is also to respond to the issue of the problem of leaking personal data of citizens in carrying out economic activities.	

In essence, the development of personal data has been adopted in various countries. However, perfection in the implementation and adoption of provisions regarding personal data is still not perfect enough to be carried out evenly and one concept. It can be seen from the two countries (China and the European Union) in this case trying to provide protection to citizens both in any form and all activities, especially against economic activity. Indonesia in this case needs to review whether the rules it makes have complied with the rules and also the provisions of personal data protection.

The form of protection of citizen data in this case must be carried out in accordance with the rules of personal data protection. Every legislation made by the government in this case must contain legal rules of formation and principles of personal data protection. The principles include:[25]

a) Collection Limitation Principles, is a principle that explains the obligation that arises to limit information that has been collected from the owner of the data. This restriction aims to prevent the acquisition of personal data from every citizen in vain.
b) The Purposes Specification Principles, is a principle that gives birth to a new obligation to explain and also describe and notify the purpose and purpose of collecting personal data belonging to the citizen.
c) The Use Limitation Principles, is a principle that also explains the existence of a new obligation to maintain confidentiality and also upholds the principle of not disseminating personal data belonging to the citizen. Not only that, other than to maintain the confidentiality of personal data, available or used for purposes other

[25] *Ibid.*, 151.

than those specified except: (a) with the consent of the data subject; or (b) by legal authorities. This means that if the personal data wants to be followed up or handed over to another party, in this case it requires an obligation of consent from the party concerned regarding whether the personal data may be disseminated or not.

d) The principle of Security, in the principle of personal data protection presents a new obligation and responsibility regarding paying attention to the element of confidentiality and also security of personal data from attacks by third parties or parties outside the personal data protection agreement which is not given permission also by the organizer. Any suspicious activities and experiments in this case the government anticipates by providing security forces through verification of the data.[26]

The national legal system in providing personal data protection to its citizens has tried its best with the limitation of PDP Law and also Regulation of Minister of Communication and Information Number 20 of 2016 on Personal Data Protection in Electronic Systems. The national legal regulations formed in this case have sought to provide legal certainty to citizens, as well as Article 2 Paragraph (1) of Regulation of Minister of Communication and Information Number 20 of 2016 on Personal Data Protection in Electronic Systems which states that "Protection of Personal Data in Electronic Systems includes protection against the acquisition, collection, processing, analysis, storage, display, announcement, transmission, dissemination and destruction of Personal Data."

The article is an affirmation that in terms of providing personal data protection, it includes the acquisition of personal data. Then, Article 26 of Minister of Communication and Information Number 20 of 2016 states that the owner of personal data has rights over himself and over the personal data he has. The article states that:

> "The Owner of Personal Data has the right: a. to the confidentiality of his/her Personal Data; b. file a complaint in the context of resolving Personal Data disputes for failure to protect the confidentiality of their Personal Data by the Electronic System Operator to the Minister; c. gain access or opportunity to change or update his/her Personal Data without disturbing the Personal Data management system, unless otherwise stipulated by the provisions of laws and regulations; d. gain access or opportunity to obtain historical Personal Data that has been submitted to the Electronic System Operator as long as it is still in accordance with the provisions of laws and regulations; and e. request the destruction of certain personal data in the Electronic System managed by the Electronic System Operator, unless otherwise stipulated by the provisions of laws and regulations"

However, with the cases of personal data breaches that exist in Indonesia today after the birth of PDP Law and Regulation of Minister of Communication and Information Number 20 of 2016 shows that the current national law does not actually provide legal protection and certainty for citizens.

This is because although the laws and regulations made in this case are in accordance with applicable legal rules, in its implementation these regulations are still difficult to implement and have not been effectively implemented. The legal sanctions given to cases against BSI are not carried out in such a way as described in PDP Law and Regulation of Minister of Communication and Information Number 20 of 2016. This shows that national laws and positive data protection laws are like only laws that have no binding legal force to

---

[26] Soediro, "Legal Relations and Globalization: Efforts to Anticipate Their Negative Impacts," *Journal of Legal Cosmic* 17, no. 1 (2017): 1.

enforce. The government should create laws that can be applied and implemented by its citizens so that in its implementation the purpose and essence of forming the law is beneficial. Not only that, in the midst of the development of cross-border cybercrime, in this case, it continues to grow, including in the realm of ransomware attack crimes, so it requires cooperation between countries to overcome this. This is related to Mutual Legal Assistance (MLA). The cooperation was formed through the establishment of an international agreement that discusses the MLA study between countries. One form of cooperation in conducting MLA relations is regulated by agreement in which it discusses the rules that allow it to be used as a hiding place or store assets from the proceeds of crime. Such cooperation can be in the form of searching, blocking, confiscating, checking letters, taking other information, and also assisting in the process of convicting and returning suspected perpetrators of crimes.[27] Indonesia needs to ratify the convention considering the need for cybercrime that continues to occur and is transnational in nature.[28]

4. CONCLUSION

Based on the description and explanation above, it can be concluded that in this case the government has tried to form data protection laws, especially personal data for its citizens through PDP Law and Regulation of Minister of Communication and Information Number 20 of 2016. However, in its implementation, the regulation is still not perfectly implemented and is used as a reference to provide data protection and privacy rights to citizens. This can be seen in the case of data leakage that occurred at BSI where BSI in this case has been proven to have committed actions that are considered unlawful against BSI Customers. This is because in its efforts BSI cannot provide protection for personal data belonging to BSI customers both which are part of the personal rights of each BSI customer as mandated by PDP Law and Regulation of Minister of Communication and Information Number 20 of 2016. For these unlawful acts, BSI customers can then file legal remedies in alternative dispute resolution processes or through litigation efforts by filing a lawsuit against the law to the district court where BSI is located. Then, the advice that can be given in the issue of personal data leakage is that the government in forming national laws related to data protection must be able to ensure effectiveness in implementing the law.

REFERENCES

Law and Regulations:

The 1945 Constitution of the Republic of Indonesia.

Law Number 19 of 2016 on Amendments to Law Number 11 of 2008 on Electronic Information and Transactions. State Gazette of the Republic of Indonesia of 2016 Number 251, Supplement to the State Gazette of the Republic of Indonesia Number 5952.

---

27 Bambang Hartono and Recca Ayu Hapsari, "Mutual Legal Assistance Pada pemberantasan Cyber Crime Lintas Yurisdiksi di Indonesia [Mutual Legal Assistance on Cross-Jurisdictional Cyber Crime Eradication in Indonesia]," *SASI* 25, no. 1 (August 2019): 59–71, https://doi.org/10.47268/sasi.v25i1.136.

28 Muhamad Amirulloh, Ida Padmanegara, and Tyas Dian Anggraeni, "Kajian EU Convention on Cybercrime Dikaitkan Dengan Upaya Regulasi Tindak Pidana Teknologi Informasi [EU Convention Cybercrime Study Linked to Information Technology Crime Regulation Efforts]" (final research report for Badan Pembinaan Hukum Nasional Departemen Hukum dan Hak Asasi Manusia RI, Jakarta, 2016).

Government Regulation Number 80 of 2019 on Trading Through Electronic Systems. State Gazette of the Republic of Indonesia of 2019 Number 222, Supplement to the State Gazette of the Republic of Indonesia Number 6420.

Regulation of Minister of Communication and Information Number 20 of 2016 on Personal Data Protection in Electronic Systems. State News of the Republic of Indonesia of 2016 Number 1829.

Books:

Derita, Prapti Rahayu. *Metode Penelitian Hukum [Legal Research Methods]*. Yogyakarta: Thafa Media, 2020.

Endeshaw, Assafa. *Hukum E-Commerce dan Internet dengan Fokus di Asia Pasifik [E-Commerce and Internet Law with a Focus on Asia Pacific]*. Surabaya: Bina Ilmu, 2007.

Fajar ND, Mukti, and Yulianto Achmad. *Dualisme Penelitian Hukum Normatif & Empiris [Dualism of Normative and Empirical Legal Research]*. Yogyakarta: Pustaka Belajar, 2015.

Hasim, Mohd. Safar. *Mengenali Undang-Undang Media dan Siber [Regarding Media and Cyber Law]*. Kuala Lumpur: Utusan Publications & Distributions, 2002.

Indrajit, Richardus Eko. *Cyber Resilience: A Holistic Strategy to Address Contemporary Defense Threats in Cyberspace*. Jakarta: BSSN, 2019.

Makarim, Edmon. *Kompilasi Hukum Telematika [Telematics Law Compilation]*. Jakarta: Raja Grafindo, 2003.

Marzuki, Peter Mahmud. *Penelitian Hukum [Legal Research]*. Jakarta: Kencana, 2007.

Ramli, Ahmad M. *Cyber Law and HAKI dalam Sistem Hukum Indonesia [Cyber Law and IPR in the Indonesian Legal System]*. Jakarta: Refika Aditama, 2020.

Situmeang, Sahat Maruli T. *Cyber Law*. Jakarta: Cakra, 2020.

Subekti, R., and R. Tjitrosudibio. *Kitab Undang-Undang Hukum Perdata [Indonesian Civil Code]*. Jakarta: Pradnya Paramitha, 2002.

Journal Articles:

Djafar, Wahyudi, and M. Jodi Santoso. "Personal Data Protection Recognizes the Rights of Data Subjects, as well as the Obligations of Data Controllers and Processors." *ELSAM Publication Journal* (2020).

Hartono, Bambang, and Recca Ayu Hapsari. "Mutual Legal Assistance Pada pemberantasan Cyber Crime Lintas Yurisdiksi di Indonesia [Mutual Legal Assitance on Cross-Jurisdictional Cyber Crime Eradication in Indonesia]." *SASI* 25, no. 1 (August 2019): 59–71. https://doi.org/10.47268/sasi.v25i1.136.

Hussain, Mubashir, and Jatinder Manhas. "Artificial Intelligence for Big Data: Potential and Relevance." *International Academy of Engineering and Medical Research* 1, no. 1 (2016): 1–5. https://www.researchgate.net/publication/310447985.

Njotorahardjo, Felicia. "Manajemen Komunikasi Privasi Seorang Mantan Pria Simpanan [anagement of Privacy Communication of a Mistress]." *Jurnal E-Komunikasi* 2, no. 3 (2014): 1–11. https://publication.petra.ac.id/index.php/ilmu-komunikasi/article/view/3813.

Soediro. "Legal Relations and Globalization: Efforts to Anticipate Their Negative Impacts." *Journal of Legal Cosmic* 17, no. 1 (2017): 1–15.

Yuniarti, Siti. "Perlindungan Hukum Data Pribadi di Indonesia [Legal Protection of Personal Data in Indonesia]." *Business Economic, Communication, and Social Sciences Journal (BECOSS)* 1, no. 1 (2019): 147–154. https://doi.org/10.21512/becossjournal.v1i1.6030

Thesis:

Jubhari, Andi Rian. "Tinjauan Hukum Pidana Internasional Terhadap Serangan Siber Menggunakan Virus Ransomware WannaCry di Indonesia [International Criminal Law Analysis of Cyberattacks Using Wannacry Ransomware Virus in Indonesia]" Undergraduate thesis, Universitas Hasanuddin, 2022. Hasanuddin Repository. https://repository.unhas.ac.id/id/eprint/12272/.

Scientific Papers:

Amirulloh, Muhamad, Ida Padmanegara, and Tyas Dian Anggraeni. "Kajian EU Convention on Cybercrime Dikaitkan Dengan Upaya Regulasi Tindak Pidana Teknologi Informasi [EU Convention Cybercrime Study Linked to Information Technology Crime Regulation Efforts]." Final Research Report for Badan Pembinaan Hukum Nasional Departemen Hukum dan Hak Asasi Manusia RI. Jakarta, 2016.

Internet:

Shidarta. "The role of the state in responding to investment according to the theory of interest of the pound." *Binus University Business Law*, January 2016. https://business-law.binus.ac.id/2016/01/03/peran-negara-dalam-menyikapi-investasi-teori-kepentingan-pound/.